

US5915019: Systems and methods for secure transaction management and electronic rights protection

[View Images \(317 pages\)](#) | [Expand Details](#) | [View Cart](#) | [View INPADOC only](#) | [Derwent Record...](#)

[Add to cart: PDF \(~30100 KB\)](#) | [TIFF](#) | [Fax](#) | [SmartPatent](#) | [File History](#) | [More choices...](#)

Inventor(s): **Ginter; Karl L.** , Beltsville, MD
Shear; Victor H. , Bethesda, MD
Spahn; Francis J. , El Cerrito, CA
Van Wie; David M. , Sunnyvale, CA

Applicant(s): **InterTrust Technologies Corp.**, Sunnyvale, CA
[News, Profiles, Stocks and More about this company](#)

Issued/Filed Dates: **June 22, 1999 / Jan. 8, 1997**


Application Number: **US1997000780393**

IPC Class: **H04L 9/00;**

ECLA Code: **G07F17/16; H04N7/24T4; H04L29/06C6C2; H04N7/24T6; G06F1/00N7R2; G07F7/10F6; H04L29/06C6B;**

Class: **Current: 705/054; 705/026; 705/400; 713/200;**
Original: 380/004; 380/021; 380/049; 395/680; 705/026; 705/400;

Field of Search: **380/3,4,5,21,49 395/680,683 705/26,400**

Legal Status:  [Show legal status actions](#)

Abstract:

Patent Playties

The present invention provides systems and methods for secure transaction management and electronic rights protection. Electronic appliances such as computers equipped in accordance with the present invention help to ensure that information is accessed and used only in authorized ways, and maintain the integrity, availability, and/or confidentiality of the information. Such electronic appliances provide a distributed virtual distribution environment (VDE) that may enforce a secure chain of handling and control, for example, to control and/or meter or otherwise monitor use of electronically stored or disseminated information. Such a virtual distribution environment may be used to protect rights of various participants in electronic commerce and other electronic or electronic-facilitated transactions. Distributed and other operating systems, environments and architectures, such as, for example, those using tamper-resistant hardware-based processors, may establish security at each node. These techniques may be used to support an all-

electronic information distribution, for example, utilizing the "electronic highway."

Attorney, Agent, or
Firm:
Primary/Assistant
Examiners:

Nixon & Vanderhye P.C.;

Barron, Jr.; Gilberto;

Related Applications:

Application Number	AppDate	Patent	Issued	Title
US1995000388107	1995-02-13			

Family: Show known family members

U.S. References:

Show the 5 patents that reference this one

Patent	Issued	Inventor(s)	Applicant(s)	Title
US3573747	4 /1971	Adams et al.	Institutional Networks Corporation	INSTINET COMMUNICATION SYSTEM FOR EFFECTUATING THE SALE OR EXCHANGE OF FUNGIBLE PROPERTIES BETWEEN SUBSCRIBERS
US3609697	9 /1971	Blevins	International Business Machines Corporation	PROGRAM SECURITY DEVICE
US3796830	3 /1974	Smith	International Business Machines Corporation	RECIRCULATING BLOCK CIPHER CRYPTOGRAPHIC SYSTEM
US3798359	3 /1974	Feistel	International Business Machines Corporation	BLOCK CIPHER CRYPTOGRAPHIC SYSTEM
US3798360	3 /1974	Feistel	International Business Machines Corporation	STEP CODE CIPHERING SYSTEM
US3798605	3 /1974	Feistel	International Business Machines Corporation	CENTRALIZED VERIFICATION SYSTEM
US3806882	4 /1974	Clarke		SECURITY FOR COMPUTER SYSTEMS
US3829833	8 /1974	Freeny, Jr.	Information Identification Company, Inc.	CODE ELEMENT IDENTIFICATION METHOD AND APPARATUS
US3906448	9 /1975	Henriques	RCA Corporation	Fault detection facilitating means for card reader of identification card reading system
US3911397	10 /1975	Freeny, Jr.	Information Identification Inc.	Access control assembly
US3924065	12 /1975	Freeny, Jr.	Information Identification, Inc.	Coherent, fixed BAUD rate FSK communication method and apparatus
US3931504	1 /1976	Jacoby	Basic Computing Arts, Inc.	Electronic data processing security system and method
US3946220	3 /1976	Brobeck et al.	Transactron, Inc.	Point-of-sale system and apparatus
US3956615	5 /1976	Anderson et al.	IBM Corporation	Transaction execution system with secure data storage and

		al.		storage and communications
US3958081	5 /1976	Ehrsam et al.	International Business Machines Corporation	Block cipher system for data security
US3970992	7 /1976	Boothroyd et al.	IBM Corporation	Transaction terminal with unlimited range of functions
US4048619	9 /1977	Forman, Jr. et al.	Digital Data Inc.	Secure two channel SCA broadcasting system
US4071911	1 /1978	Mazur	Continental Can Co. Inc.	Machine control system with machine serializing and safety circuits
US4112421	9 /1978	Freeny, Jr.	Information Identification Company, Inc.	Method and apparatus for automatically monitoring objects
US4120030	10 /1978	Johnstone	Kearney & Trecker Corporation	Computer software security system
US4163280	7 /1979	Mori et al.	Tokyo Shibaura Electric Co., Ltd.	Address management system
US4168396	9 /1979	Best		Microprocessor for executing enciphered programs
US4196310	4 /1980	Forman et al.	Digital Data, Inc.	Secure SCA broadcasting system including subscriber actuated portable receiving terminals
US4200913	4 /1980	Kuhar et al.	International Business Machines Corporation	Operator controlled programmable keyboard apparatus
US4209787	6 /1980	Freeny, Jr.	Gould Inc.	Method for monitoring the location of monitored objects
US4217588	8 /1980	Freeny, Jr.	Information Identification Company, Inc.	Object monitoring method and apparatus
US4220991	9 /1980	Hamano et al.	Tokyo Electric Co., Ltd.	Electronic cash register with removable memory packs for cashier identification
US4232193	11 /1980	Gerard	The Marconi Company Limited	Message signal scrambling apparatus
US4232317	11 /1980	Freeny, Jr.		Quantized hyperbolic and inverse hyperbolic object location system
US4236217	11 /1980	Kennedy		Energy utilization or consumption recording arrangement
US4253157	2 /1981	Kirschner et al.	Alpex Computer Corp.	Data access system wherein subscriber terminals gain access to a data bank by telephone lines
US4262329	4 /1981	Bright et al.	Computation Planning, Inc.	Security system for data processing
US4265371	5 /1981	Desai et al.	Trafalgar Industries Inc.	Foodstuff vending apparatus employing improved solid-state type control apparatus
US4270182	5 /1981	Asija		Automated information input, storage, and

				<u>retrieval system</u>
<u>US4278837</u>	7 /1981	Best		<u>Crypto microprocessor for executing enciphered programs</u>
<u>US4305131</u>	12 /1981	Best		<u>Dialog between TV movies and human viewers</u>
<u>US4306289</u>	12 /1981	Lumley	Western Electric Company, Inc.	<u>Digital computer having code conversion apparatus for an encrypted program</u>
<u>US4309569</u>	1 /1982	Merkle	The Board of Trustees of the Leland Stanford Junior University	<u>Method of providing digital signatures</u>
<u>US4319079</u>	3 /1982	Best		<u>Crypto microprocessor using block cipher</u>
<u>US4323921</u>	4 /1982	Guillou	Etablissement Public de Diffusion dit "Telediffusion de France"	<u>System for transmitting information provided with means for controlling access to the information transmitted</u>
<u>US4328544</u>	5 /1982	Baldwin et al.	International Business Machines Corporation	<u>Electronic point-of-sale system using direct-access storage</u>
<u>US4337483</u>	6 /1982	Guillou	Etablissement Public de Diffusion dit "Telediffusion de France"	<u>Text video-transmission system provided with means for controlling access to the information</u>
<u>US4361877</u>	11 /1982	Dyer et al.	Sangamo Weston, Inc.	<u>Billing recorder with non-volatile solid state memory</u>
<u>US4375579</u>	3 /1983	Davida et al.	Wisconsin Alumni Research Foundation	<u>Database encryption and decryption circuit and method using subkeys</u>
<u>US4433207</u>	2 /1984	Best		<u>Cryptographic decoder for computer programs</u>
<u>US4434464</u>	2 /1984	Suzuki et al.	Hitachi, Ltd.	<u>Memory protection system for effecting alteration of protection information without intervention of control program</u>
<u>US4442486</u>	4 /1984	Mayer	U.S. Philips Corporation	<u>Protected programmable apparatus</u>
<u>US4446519</u>	5 /1984	Thomas	Corban International, Ltd.	<u>Method and apparatus for providing security for computer software</u>
<u>US4454594</u>	6 /1984	Heffron et al.	U.S. Philips Corporation	<u>Method and apparatus to secure proprietary operation of computer equipment</u>
<u>US4458315</u>	7 /1984	Uchenick	Penta, Inc.	<u>Apparatus and method for preventing unauthorized use of computer programs</u>
<u>US4462076</u>	7 /1984	Smith, III	Smith Engineering	<u>Video game cartridge recognition and security system</u>
<u>US4462078</u>	7 /1984	Ross		<u>Computer program protection method</u>
<u>US4465901</u>	8 /1984	Best		<u>Crypto microprocessor that executes enciphered programs</u>
<u>US4471163</u>	9 /1984	Donald et al.		<u>Software protection system</u>
				<u>Method and system for</u>

US4484217	11 /1984	Block et al.	Telease, Inc.	remote reporting, particularly for pay television billing
US4494156	1 /1985	Kadison et al.	Media Systems Technology	Selectable format computer disk copier machine
US4513174	4 /1985	Herman	Standard Microsystems Corporation	Software security method using partial fabrication of proprietary control word decoders and microinstruction memories
US4528588	7 /1985	Lofberg		Method and apparatus for marking the information content of an information carrying signal
US4528643	7 /1985	Freeny, Jr.	FPDC, Inc.	System for reproducing information in material objects at a point of sale location
US4553252	11 /1985	Egendorf		Counting computer software cartridge
US4558176	12 /1985	Arnold et al.		Computer systems to inhibit unauthorized copying, unauthorized usage, and automated cracking of protected software
US4558413	12 /1985	Schmidt et al.	Xerox Corporation	Software version management system
US4562306	12 /1985	Chou et al.		Method and apparatus for protecting computer software utilizing an active coded hardware device
US4562495	12 /1985	Bond et al.	Verbatim Corporation	Multiple system disk
US4577289	3 /1986	Comerford et al.	International Business Machines Corporation	Hardware key-on-disk system for copy-protecting magnetic storage media
US4584641	4 /1986	Guglielmino		Copyprotecting system for software protection
US4588991	5 /1986	Atalla	Atalla Corporation	File access security method and means
US4589064	5 /1986	Chiba et al.	Fujitsu Limited	System for controlling key storage unit which controls access to main storage
US4593353	6 /1986	Pickholtz	Telecommunications Associates, Inc.	Software protection method and apparatus
US4593376	6 /1986	Volk		System for vending program cartridges which have circuitry for inhibiting program usage after preset time interval expires
US4595950	6 /1986	Lofberg		Method and apparatus for marking the information content of an information carrying signal
US4597058	6 /1986	Izumi et al.	Romox, Inc.	Cartridge programming system
US4634807	1 /1987	Chorley et al.	National Research Development Corp.	Software protection device
			International	Implementing a shared higher level of privilege on

US4644493	2 /1987	Chandra et al.	Business Machines Corporation	higher level of privilege on personal computers for copy protection of software
US4646234	2 /1987	Tolman et al.	Brigham Young University	Anti-piracy system using separate storage and alternate execution of selected proprietary and public portions of computer programs
US4652990	3 /1987	Pailen et al.	Remote Systems, Inc.	Protected software access control apparatus and method
US4658093	4 /1987	Hellman		Software distribution system
US4670857	6 /1987	Rackman		Cartridge-controlled system whose use is limited to authorized cartridges
US4672572	6 /1987	Alsberg	Gould Inc.	Protector system for computer access and use
US4677434	6 /1987	Fascenda	Lotus Information Network Corp.	Access control system for transmitting data from a central station to a plurality of receiving stations and method therefor
US4680731	7 /1987	Izumi et al.	Romox Incorporated	Reprogrammable cartridge memory with built-in identification circuitry and programming method
US4683553	7 /1987	Mollier	Cii Honeywell Bull (Societe Anonyme)	Method and device for protecting software delivered to a user by a supplier
US4685056	8 /1987	Barnsdale et al.	Pueblo Technologies, Inc.	Computer security device
US4688169	8 /1987	Joshi		Computer software security system
US4691350	9 /1987	Kleijne et al.	NCR Corporation	Security device for stored sensitive data
US4696034	9 /1987	Wiedemer	Signal Security Technologies	High security pay television system
US4701846	10 /1987	Ikeda et al.	Panafacom Limited	Computer system capable of interruption using special protection code for write interruption region of memory device
US4712238	12 /1987	Gilhousen et al.	M/A-COM Government Systems, Inc.	Selective-subscription descrambling
US4713753	12 /1987	Boebert et al.	Honeywell Inc.	Secure data processing system architecture with format control
US4740890	4 /1988	William	Software Concepts, Inc.	Software protection system with trial period usage code and unlimited use unlocking code both recorded on program storage media
US4747139	5 /1988	Taaffe		Software security method and systems
US4757533	7 /1988	Allen et al.	Computer Security Corporation	Security system for microcomputers

<u>US4757534</u>	7 /1988	Matyas et al.	International Business Machines Corporation	<u>Code protection using cryptography</u>
<u>US4768087</u>	8 /1988	Taub et al.	National Information Utilities Corporation	<u>Education utility</u>
<u>US4791565</u>	12 /1988	Dunham et al.	Effective Security Systems, Inc.	<u>Apparatus for controlling the use of computer software</u>
<u>US4796181</u>	1 /1989	Wiedemer		<u>Billing system for computer software</u>
<u>US4799156</u>	1 /1989	Shavit et al.	Strategic Processing Corporation	<u>Interactive market management system</u>
<u>US4807288</u>	2 /1989	Ugon et al.	C.I.I. Honeywell Bull	<u>Microprocessor intended particularly for executing the calculation algorithms of a public code encoding system</u>
<u>US4817140</u>	3 /1989	Chandra et al.	International Business Machines Corp.	<u>Software protection system using a single-key cryptosystem, a hardware-based authorization system and a secure coprocessor</u>
<u>US4823264</u>	4 /1989	Deming		<u>Electronic funds transfer system</u>
<u>US4827508</u>	5 /1989	Shear	Personal Library Software, Inc.	<u>Database usage metering and protection system and method</u>
<u>US4858121</u>	8 /1989	Barber et al.	Medical Payment Systems, Incorporated	<u>Medical payment system</u>
<u>US4864494</u>	9 /1989	Kobus	Computerized Data Ssystems for Mfg., Inc.	<u>Software usage authorization system with key for decrypting/re-encrypting/re-transmitting moving target security codes from protected software</u>
<u>US4868877</u>	9 /1989	Fischer		<u>Public key/signature cryptosystem with enhanced digital signature certification</u>
<u>US4903296</u>	2 /1990	Chandra et al.	International Business Machines Corporation	<u>Implementing a shared higher level of privilege on personal computers for copy protection of software</u>
<u>US4924378</u>	5 /1990	Hershey et al.	Prime Computer, Inc.	<u>License mangagement system and license storage key</u>
<u>US4930073</u>	5 /1990	Cina, Jr.	International Business Machines Corporation	<u>Method to prevent use of incorrect program version in a computer system</u>
<u>US4949187</u>	8 /1990	Cohen		<u>Video communications system having a remotely controlled central source of video and audio data</u>
<u>US4977594</u>	12 /1990	Shear	Electronic Publishing Resources, Inc.	<u>Database usage metering and protection system and method</u>
<u>US4999806</u>	3 /1991	Chernow et al.		<u>Software distribution system</u>

<u>US5001752</u>	3 /1991	Fischer		Public/key date-time notary facility
<u>US5005122</u>	4 /1991	Griffin et al.	Digital Equipment Corporation	Arrangement with cooperating management server node and network service node
<u>US5005200</u>	4 /1991	Fischer		Public key/signature cryptosystem with enhanced digital signature certification
<u>US5010571</u>	4 /1991	Katznelson	Titan Linkabit Corporation	Metering retrieval of encrypted data stored in customer data retrieval terminal
<u>US5023907</u>	6 /1991	Johnson et al.	Apollo Computer, Inc.	Network license server
<u>US5047928</u>	9 /1991	Wiedemer		Billing system for computer software
<u>US5048085</u>	9 /1991	Abraham et al.	International Business Machines Corporation	Transaction system security method and apparatus
<u>US5050213</u>	9 /1991	Shear	Electronic Publishing Resources, Inc.	Database usage metering and protection system and method
<u>US5091966</u>	2 /1992	Bloomberg et al.	Xerox Corporation	Adaptive scaling for decoding spatially periodic self-clocking glyph shape codes
<u>US5103392</u>	4 /1992	Mori	Fujitsu Limited	System for storing history of use of programs including user credit data and having access by the proprietor
<u>US5103476</u>	4 /1992	Waite et al.		Secure system for activating personal computer software at remote locations
<u>US5111390</u>	5 /1992	Ketcham	Unisys Corporation	Software security system for maintaining integrity of compiled object code by restricting users ability to define compilers
<u>US5119493</u>	6 /1992	Janis et al.	International Business Machines Corporation	System for recording at least one selected activity from a selected resource object within a distributed data processing system
<u>US5128525</u>	7 /1992	Stearns et al.	Xerox Corporation	Convolution filtering for decoding self-clocking glyph shape codes
<u>US5136643</u>	8 /1992	Fischer		Public/key date-time notary facility
<u>US5136646</u>	8 /1992	Haber et al.	Bell Communications Research, Inc.	Digital document time-stamping with catenate certificate
<u>US5136647</u>	8 /1992	Haber et al.	Bell Communications Research, Inc.	Method for secure time-stamping of digital documents
<u>US5136716</u>	8 /1992	Harvey et al.	Digital Equipment Corporation	Session control in network for digital data processing system which supports multiple transfer protocols

US5146575	9 /1992	Nolan, Jr.	International Business Machines Corp.	Implementing privilege on microprocessor systems for use in software asset protection
US5148481	9 /1992	Abraham et al.	International Business Machines Corporation	Transaction system security method and apparatus
US5155680	10 /1992	Wiedemer	Signal Security Technologies	Billing system for computing software
US5168147	12 /1992	Bloomberg	Xerox Corporation	Binary image processing for decoding self-clocking glyph shape codes
US5185717	2 /1993	Mori		Tamper resistant module having logical elements arranged in multiple layers on the outer surface of a substrate to protect stored information
US5201046	4 /1993	Goldberg et al.	Xidak, Inc.	Relational database management system and method for storing, retrieving and modifying directed graph data structures
US5201047	4 /1993	Maki et al.	International Business Machines Corporation	Attribute-based classification and retrieval system
US5208748	5 /1993	Flores et al.	Action Technologies, Inc.	Method and apparatus for structuring and managing human communications by explicitly defining the types of communications permitted between participants
US5214702	5 /1993	Fischer		Public key/signature cryptosystem with enhanced digital signature certification
US5216603	6 /1993	Flores et al.	Action Technologies, Inc.	Method and apparatus for structuring and managing human communications by explicitly defining the types of communications permitted between participants
US5221833	6 /1993	Hecht	Xerox Corporation	Methods and means for reducing bit error rates in reading self-clocking glyph codes
US5222134	6 /1993	Waite et al.	Tau Systems Corporation	Secure system for activating personal computer software at remote locations
US5224160	6 /1993	Paulini et al.	Siemens Nixdorf Informationssysteme AG	Process for securing and for checking the integrity of the secured programs
US5224163	6 /1993	Gasser et al.	Digital Equipment Corporation	Method for delegating authorization from one entity to another through the use of session encryption keys
			Digital Equipment	Access control subsystem and method for distributed

US5235642	8 /1993	Wobber et al.	Digital Equipment Corporation	computer system using locally cached authentication credentials
US5245165	9 /1993	Zhang	Xerox Corporation	Self-clocking glyph code for encoding dual bit digital values robustly
US5247575	9 /1993	Sprague et al.		Information distribution system
US5260999	11 /1993	Wyman	Digital Equipment Corporation	Filters in license management system
US5263158	11 /1993	Janis	International Business Machines Corporation	Method and system for variable authority level user access control in a distributed data processing system having multiple resource manager
US5265164	11 /1993	Matyas et al.	International Business Machines Corporation	Cryptographic facility environment backup/restore and replication in a public key cryptosystem
US5276735	1 /1994	Boebert et al.	Secure Computing Corporation	Data enclave and trusted path system
US5280479	1 /1994	Mary	Matra Communication	Device for insertion of digital packets in a transmission channel
US5285494	2 /1994	Sprecher et al.	PacTel Corporation	Network management system
US5301231	4 /1994	Abraham	International Business Machines Corporation	User defined function facility
US5311591	5 /1994	Fischer		Computer system security method and apparatus for creating and using program authorization information data structures
US5319705	6 /1994	Halter et al.	International Business Machines Corporation	Method and system for multimedia access control enablement
US5337360	8 /1994	Fischer		Method and apparatus for creating, supporting, and using travelling programs
US5341429	8 /1994	Stringer et al.	TestDrive Corporation	Transformation of ephemeral material
US5343527	8 /1994	Moore	International Business Machines Corporation	Hybrid encryption method and system for protecting reusable software components
US5347579	9 /1994	Blandford		Personal computer diary
US5351293	9 /1994	Michener et al.	Wave Systems Corp.	System method and apparatus for authenticating an encrypted signal
US5355474	10 /1994	Thuraisingham et al.		System for multilevel secure database management using a knowledge base with release-based and other security constraints for query, response and update modification
			Bell	Method of extending the validity of a cryptographic

<u>US5373561</u>	12 /1994	Haber et al.	Communications Research, Inc.	<u>validity of a cryptographic certificate</u>
<u>US5390247</u>	2 /1995	Fischer		<u>Method and apparatus for creating, supporting, and using travelling programs</u>
<u>US5390330</u>	2 /1995	Talati		<u>Control system and method for direct execution of software application information models without code generation</u>
<u>US5392220</u>	2 /1995	van den Hamer et al.	U.S. Philips Corporation	<u>Method and system for organizing data</u>
<u>US5392390</u>	2 /1995	Crozier	IntelliLink Corp.	<u>Method for mapping, translating, and dynamically reconciling data between disparate computer platforms</u>
<u>US5394469</u>	2 /1995	Nagel et al.	Infosafe Systems, Inc.	<u>Method and apparatus for retrieving secure information from mass storage media</u>
<u>US5410598</u>	4 /1995	Shear	Electronic Publishing Resources, Inc.	<u>Database usage metering and protection system and method</u>
<u>US5412717</u>	5 /1995	Fischer		<u>Computer system security method and apparatus having program authorization information data structures</u>
<u>US5421006</u>	5 /1995	Jablon	Compaq Computer Corp.	<u>Method and apparatus for assessing integrity of computer system software</u>
<u>US5422953</u>	6 /1995	Fischer		<u>Personal date/time notary device</u>
<u>US5428606</u>	6 /1995	Moskowitz		<u>Digital information commodities exchange</u>
<u>US5438508</u>	8 /1995	Wyman	Digital Equipment Corporation	<u>License document interchange format for license management system</u>
<u>US5442645</u>	8 /1995	Ugon	Bull CP8	<u>Method for checking the integrity of a program or data, and apparatus for implementing this method</u>
<u>US5444779</u>	8 /1995	Daniele	Xerox Corporation	<u>Electronic copyright royalty accounting system using glyphs</u>
<u>US5449895</u>	9 /1995	Hecht et al.	Xerox Corporation	<u>Explicit synchronization for self-clocking glyph codes</u>
<u>US5449896</u>	9 /1995	Hecht et al.	Xerox Corporation	<u>Random access techniques for use with self-clocking glyph codes</u>
<u>US5450493</u>	9 /1995	Maher	AT&T Corp.	<u>Secure communication method and apparatus</u>
<u>US5453601</u>	9 /1995	Rosen	Citibank, N.A.	<u>Electronic-monetary system</u>
<u>US5453605</u>	9 /1995	Hecht et al.	Xerox Corporation	<u>Global addressability for self-clocking glyph codes</u>
<u>US5455407</u>	10 /1995	Rosen	Citibank, N.A.	<u>Electronic-monetary system</u>
<u>US5455861</u>	10 /1995	Faucher et al.	AT&T Corp.	<u>Secure</u>

US5455861	10 /1995	Faucher et al.	AT&T Corp.	telecommunications
US5455953	10 /1995	Russell	Wang Laboratories, Inc.	Authorization system for obtaining in single step both identification and access rights of client to server directly from encrypted authorization ticket
US5457746	10 /1995	Dolphin	Spyrus, Inc.	System and method for access control for portable data storage media
US5463565	10 /1995	Cookson et al.	Time Warner Entertainment Co., L.P.	Data block format for software carrier and player therefor
US5473687	12 /1995	Lipscomb et al.	Infosafe Systems, Inc.	Method for retrieving secure information from a database
US5473692	12 /1995	Davis	Intel Corporation	Roving software license for a hardware agent
US5479509	12 /1995	Ugon	Bull CP8	Method for signature of an information processing file, and apparatus for implementing it
US5485622	1 /1996	Yamaki	Kabushiki Kaisha Toshiba	Password processing system for computer
US5491800	2 /1996	Goldsmith et al.	Taligent, Inc.	Object-oriented remote procedure call networking system
US5497479	3 /1996	Hornbuckle	Softel, Inc.	Method and apparatus for remotely controlling and monitoring the use of computer software
US5497491	3 /1996	Mitchell et al.	International Business Machines Corporation	System and method for importing and exporting data between an object oriented computing environment and an external computing environment
US5499298	3 /1996	Narasimhalu et al.	National University of Singapore	Controlled dissemination of digital information
US5504757	4 /1996	Cook et al.	International Business Machines Corporation	Method for selecting transmission speeds for transmitting data packets over a serial bus
US5504818	4 /1996	Okano		Information processing system using error-correcting codes and cryptography
US5504837	4 /1996	Griffeth et al.	Bell Communications Research, Inc.	Method for resolving conflicts among distributed entities through the generation of counter proposals by transversing a goal hierarchy with acceptable, unacceptable, and indeterminate nodes
US5508913	4 /1996	Yamamoto et al.	Fujitsu Limited	Electronic automatic offer matching system for freezer exchange transactions among banks
				Method for encouraging

<u>US5509070</u>	4 /1996	Schull	SoftLock Services Inc.	<u>purchase of executable and non-executable software</u>
<u>US5513261</u>	4 /1996	Maher	AT&T Corp.	<u>Key management scheme for use with electronic cards</u>
<u>US5530235</u>	6 /1996	Stefik et al.	Xerox Corporation	<u>Interactive contents revealing storage device</u>
<u>US5530752</u>	6 /1996	Rubin	Convex Computer Corporation	<u>Systems and methods for protecting software from unlicensed copying and use</u>
<u>US5533123</u>	7 /1996	Force et al.	National Semiconductor Corporation	<u>Programmable distributed personal security</u>
<u>US5534975</u>	7 /1996	Stefik et al.	Xerox Corporation	<u>Document processing system utilizing document service cards to provide document processing services</u>
<u>US5537526</u>	7 /1996	Anderson et al.	Taugent, Inc.	<u>Method and apparatus for processing a display document utilizing a system level document framework</u>
<u>US5539735</u>	7 /1996	Moskowitz		<u>Digital information commodities exchange</u>
<u>US5539828</u>	7 /1996	Davis	Intel Corporation	<u>Apparatus and method for providing secured communications</u>
<u>US5550971</u>	8 /1996	Brunner et al.	U S West Technologies, Inc.	<u>Method and system for generating a user interface adaptable to various database management systems</u>
<u>US5553282</u>	9 /1996	Parrish et al.	Taligent, Inc.	<u>Software project history database and method of operation</u>
<u>US5557518</u>	9 /1996	Rosen	Citibank, N.A.	<u>Trusted agents for open electronic commerce</u>
<u>US5563946</u>	10 /1996	Cooper et al.	International Business Machines Corporation	<u>Method and apparatus for enabling trial period use of software products: method and apparatus for passing encrypted files between data processing systems</u>
<u>US5568552</u>	10 /1996	Davis	Intel Corporation	<u>Method for providing a roving software license from one node to another node</u>
<u>US5572673</u>	11 /1996	Shurts	Sybase, Inc.	<u>Secure multi-level system for executing stored procedures</u>
<u>US5592549</u>	1 /1997	Nagel et al.	Infosafe Systems, Inc.	<u>Method and apparatus for retrieving selected information from a secure information source</u>
<u>US5606609</u>	2 /1997	Houser et al.	Scientific-Atlanta	<u>Electronic document verification system and method</u>
<u>US5613004</u>	3 /1997	Cooperman et al.	The Dice Company	<u>Steganographic method and device</u>

<u>US5621797</u>	4 /1997	Rosen	Citibank, N.A.	<u>Electronic ticket presentation and transfer method</u>
<u>US5629980</u>	5 /1997	Stefik et al.	Xerox Corporation	<u>System for controlling the distribution and use of digital works</u>
<u>US5633932</u>	5 /1997	Davis et al.	Intel Corporation	<u>Apparatus and method for preventing disclosure through user-authentication at a printing node</u>
<u>US5634012</u>	5 /1997	Stefik et al.	Xerox Corporation	<u>System for controlling the distribution and use of digital works having a fee reporting mechanism</u>
<u>US5636292</u>	6 /1997	Rhoads	Digimarc Corporation	<u>Steganography methods employing embedded calibration data</u>
<u>US5638443</u>	6 /1997	Stefik et al.	Xerox Corporation	<u>System for controlling the distribution and use of composite digital works</u>
<u>US5638504</u>	6 /1997	Scott et al.	Object Technology Licensing Corp.	<u>System and method of processing documents with document proxies</u>
<u>US5640546</u>	6 /1997	Gopinath et al.	Network Programs, Inc.	<u>Composition of systems of objects by interlocking coordination, projection, and distribution</u>
<u>US5655077</u>	8 /1997	Jones et al.	Microsoft Corporation	<u>Method and system for authenticating access to heterogeneous computing services</u>
<u>US5687236</u>	11 /1997	Moskowitz et al.	The Dice Company	<u>Steganographic method and device</u>
<u>US5689587</u>	11 /1997	Bender et al.	Massachusetts Institute of Technology	<u>Method and apparatus for data hiding in images</u>
<u>US5692180</u>	11 /1997	Lee	International Business Machines Corporation	<u>Object-oriented cell directory database for a distributed computing environment</u>
<u>US5710834</u>	1 /1998	Rhoads	Digimarc Corporation	<u>Method and apparatus responsive to a code signal conveyed through a graphic image</u>
<u>US5740549</u>	4 /1998	Reilly et al.	PointCast, Inc.	<u>Information and advertising distribution system and method</u>
<u>US5745604</u>	4 /1998	Rhoads	Digimarc Corporation	<u>Identification/authentication system using robust, distributed coding</u>
<u>US5748763</u>	5 /1998	Rhoads	Digimarc Corporation	<u>Image steganography system featuring perceptually adaptive and globally scalable signal embedding</u>
<u>US5748783</u>	5 /1998	Rhoads	Digimarc Corporation	<u>Method and apparatus for robust information coding</u>
<u>US5748960</u>	5 /1998	Fischer		<u>Method and apparatus for validating travelling object-oriented programs with digital signatures</u>

US5754849	5 /1998	Dyer et al.	Wayfarer Communications, Inc.	Self-describing object providing dynamic manipulation of heterogeneous data values and semantic identity between memory and transmission representations
US5757914	5 /1998	McManis	Sun Microsystems, Inc.	System and method for protecting use of dynamically linked executable modules
US5758152	5 /1998	LeTourneau	Prime Arithmetics, Inc.	Method and apparatus for the generation and manipulation of data structures
US5765152	1 /1998	Erickson	Trustees of Dartmouth College	System and method for managing copyrighted electronic media
US5768426	6 /1998	Rhoads	Digimarc Corporation	Graphics processing system employing embedded code signals



CLAIMS:
[Hide claims]:

We claim:

1. A method of operating on a first secure container arrangement having a first set of controls associated therewith, said first secure container arrangement at least in part comprising a first protected content file, said method comprising the following steps performed within a virtual distribution environment including at least one electronic appliance:

- using at least one control associated with said first secure container arrangement for governing, at least in part, at least one aspect of use of said first protected content file while said first protected content file is contained in said first secure container arrangement;
- creating a second secure container arrangement having a second set of controls associated therewith, said second set of controls governing, at least in part, at least one aspect of use of any protected content file contained within said second secure container arrangement;
- transferring at least a portion of said first protected content file to said second secure container arrangement, said portion made up of at least some of said first protected content file; and
- using at least one rule to govern at least one aspect of use of said first protected content file portion while said portion is contained within said second secure container arrangement;
- in which
- said first secure container arrangement comprises a third secure container arrangement comprising a third set of controls and said first protected content file, and
- said first secure container arrangement further comprises a fourth secure container arrangement comprising a fourth set of controls and a second protected content file.

2. A method as in claim 1 in which said step of creating a second secure container arrangement is governed, at least in part, by a first subset of controls contained within said first set of controls.

3. A method as in claim 1 in which said step of creating a second secure container arrangement includes a step of creating said second set of controls by copying said third set of controls.

4. A method as in claim 2 in which said step of creating a second secure container arrangement is governed in part by controls contained within said third set of controls.

5. A method as in claim 4 in which said second set of controls comprises controls copied from said first set of controls and controls copied from said third set of controls.

6. A method as in claim 5 in which said second set of controls further comprises controls not copied from either said first set of controls or said third set of controls.

7. A method as in claim 4 in which said step of creating a second secure container arrangement is governed in part by controls not contained within said first set of controls or said third set of controls.

8. A method of operating on a first secure container arrangement having a first set of controls associated therewith, said first secure container arrangement at least in part comprising a first protected content file, said method comprising the following steps performed within a virtual distribution environment including at least one electronic appliance:

- using at least one control associated with said first secure container arrangement for governing, at least in part, at least one aspect of use of said first protected content file while said first protected content file is contained in said first secure container arrangement;
- creating a second secure container arrangement having a second set of controls associated therewith said second set of controls governing, at least in part, at least one aspect of use of any protected content file contained within said second secure container arrangement;
- transferring at least a portion of said first protected content file to said second secure container arrangement said portion made up of at least some of said first protected content file; and
- using at least one rule to govern at least one aspect of use of said first protected content file portion while said portion is contained within said second secure container arrangement,
- in which said step of creating said second secure container arrangement occurs at a first site, and said step of transferring further comprises said second secure container arrangement being transferred to a second site distinct from said first site; and
- in which said first site is associated with a content distributor;
- said second site is associated with a user of content; and
- said user directly or indirectly initiating communication with said first site;
- in which said step of said user directly or indirectly initiating communication with said first site includes a step of transmitting a third secure container arrangement to said first site, said third secure container arrangement comprising a third set of controls.

9. A method as in claim 8 in which said third set of controls comprises at least a REGISTER control.

10. A method as in claim 8 in which said third set of controls comprises at least a WANT control.

11. A method as in claim 8 in which said third set of controls comprises controls specifying content desired by said user and terms under which said user is willing to obtain said content.

12. A method as in claim 11 in which said step of creating said second secure container arrangement is governed, at least in part, by controls from said first set of controls, and controls from said third set of controls.

13. A method as in claim 12 in which said second set of controls comprises controls created through an interaction between said first set of controls and said third set of controls.

14. A method as in claim 12 in which said second set of controls comprises controls copied from said first set of controls and controls copied from said third set of controls.

15. A method as in claim 13 in which said second set of controls comprises at least some controls not found in said first set of controls and said third set of controls.

16. A method as in claim 13 in which said second set of controls includes controls governing the use by said user of said first protected content file portion.

17. A method as in claim 16 in which said second set of controls includes controls governing the price to be paid by said user for use of said first protected content file portion.

18. A method as in claim 16 in which said second set of controls includes controls governing the auditing method to be used in connection with use by said user of said first protected content file portion.

19. A method as in claim 16 in which said second set of controls includes controls specifying the clearinghouse to be used for payment by said user for use of said first protected content file portion.

20. A method as in claim 16 in which said second set of controls includes controls specifying information to be provided by said user in return for use of said first protected content file portion.

21. A method of operating on a first secure container arrangement having a first set of controls associated therewith, said first secure container arrangement at least in part comprising a first protected content file, said method comprising the following steps performed within a virtual distribution environment including at least one electronic appliance:

- using at least one control associated with said first secure container arrangement for governing, at least in part, at least one aspect of use of said first protected content file while said first protected content file is contained in said first secure container arrangement;
- creating a second secure container arrangement having a second set of controls associated therewith, said second set of controls governing, at least in part, at least one aspect of use of any protected content file contained within said second secure container arrangement;
- transferring at least a portion of said first protected content file to said second secure container arrangement, said portion made up of at least some of said first protected content file; and
- using at least one rule to govern at least one aspect of use of said first protected content file portion while said portion is contained within said second secure container arrangement,
- in which said step of creating said second secure container arrangement occurs at a first site, and said step of transferring further comprises said second secure container arrangement being transferred to a second site distinct from said first site; and
- in which said first site is associated with a content distributor;
- said second site is associated with a user of content; and
- said user directly or indirectly initiating communication with said first site;
- further comprising
 - establishing a level of compensation required for said transferring step, and
 - calling a budget method to establish whether one or more budgets associated with said user are sufficient to satisfy said required compensation.

22. A method as in claim 21 further comprising

- failing to perform to said step of transferring if said budget method establishes that said one or more budgets associated with said user are not sufficient to satisfy said required compensation.

23. A method as in claim 21 in which said budget method is governed by controls contained in said first set of controls.

24. A method as in claim 21 in which said budget method is governed by controls contained in said third set of controls.

25. A method as in claim 23 in which said budget method is also governed by controls contained in said third set of controls.

26. A method of operating on a first secure container arrangement having a first set of controls associated therewith, said first secure container arrangement at least in part comprising a first protected content file, said method comprising the following steps performed within a virtual distribution environment including at least one electronic appliance:

- using at least one control associated with said first secure container arrangement for governing, at least in part, at least one aspect of use of said first protected content file while said first protected content file is contained in said first secure container arrangement;
- creating a second secure container arrangement having a second set of controls associated therewith, said second set of controls governing, at least in part, at least one aspect of use of any protected content file contained within said second secure container arrangement;
- transferring at least a portion of said first protected content file to said second secure container arrangement, said portion made up of at least some of said first protected content file; and
- using at least one rule to govern at least one aspect of use of said first protected content file portion while said portion is contained within said second secure container arrangement;
- in which said steps of transferring at least a portion of said first protected content file and creating said second secure container arrangement are governed at least in part by the same control or set of controls,
- in which said first set of controls includes controls which determine, at least in part, the permitted uses of said first protected content file while said first protected content file is contained within said first secure container arrangement
- in which said second set of controls includes controls which determine, at least in part, the permitted uses of said transferred portion of said first protected content file while said transferred portion of said first protected content file is contained within said second secure container arrangement
- in which said first set of controls includes at least a second subset of controls which determine, at least in part, the controls contained in said second set of controls; and
- in which said first secure container arrangement further comprises a third secure container arrangement.

27. A method as in claim 5 in which said creation of said second secure container arrangement further comprises using a template which specifies one or more of the controls contained in said second set of controls.

28. A method as in claim 6 in which said creation of said second secure container arrangement further comprises using a template which specifies one or more attributes of said second secure container arrangement.

29. A method as in claim 7 in which said creation of said second

secure container arrangement further comprises using a template which specifies one or more of the controls contained in said second set of controls.

30. An electronic appliance comprising:

- a memory storing a first secure container comprising a first set of rules and a first protected file;
- a secure processing unit comprising:
 - a container creator that creates a second secure container comprising a second set of rules;
 - an extractor that extracts at least a first portion of said first protected file from said first secure container;
 - a file transfer arrangement that transfers said first portion of said first protected file from said first secure container to said second secure container, said file transfer arrangement operating under the control of said first set of rules; and
 - a control element that uses said second set of rules to govern at least one operation involving said first portion of said first protected file while said first portion is contained in said second secure container;
- in which said container creator comprises:
 - means for copying at least one rule from said first set of rules; and
 - means for incorporating said at least one rule in said second set of rules,
- further comprising means by which at least one rule from said first set of rules governs said container creator,
- wherein said memory also stores a third secure container comprising a third set of rules, said first secure container being stored within said third secure container.

31. An electronic appliance as in claim 30 further comprising means by which at least one rule from said third set of rules governs said container creator.

32. An electronic appliance as in claim 31 further comprising means by which at least one rule from said third set of rules is incorporated in said second set of rules.

33. A data processing arrangement comprising at least one storing arrangement that at least temporarily stores a first secure container comprising first protected data and a first set of rules governing use of said first protected data, and at least temporarily stores a second secure container comprising second protected data different from said first protected data and a second set of rules governing use of said second protected data; and

- a data transfer arrangement, coupled to at least one storing arrangement, for transferring at least a portion of said first protected data and a third set of rules governing use of said portion of said first protected data to said second secure container,
- further comprising
 - means for creating and storing, in said at least one storing arrangement, a third secure container;
 - said data transfer arrangement further comprising means for transferring said portion of said first protected data and said third set of rules to said third secure container, and means for incorporating said third secure container within said second secure container.

34. A data processing arrangement as in claim 33 further comprising means for applying said third set of rules to govern at

least one aspect of use of said portion of said first protected data.

35. A data processing arrangement as in claim 34 further comprising means for applying said second set of rules to govern at least one aspect of use of said portion of said first protected data.

36. A method comprising the following steps:

- generating a first secure container comprising a first set of rules and a first protected file;
- generating a second secure container comprising a second set of rules and a second protected file;
- transferring a first portion of said first protected file to said second secure container, said transferring step governed by said first set of rules and comprising:
 - copying said first portion,
 - creating a third set of rules, and
 - storing said copied first portion and said third set of rules in said second secure container, and
- further comprising:
 - storing said first secure container in a memory located at a first site, and storing said second secure container in a memory located at a second site remote from said first site; and
- wherein said transferring step further comprises:
 - creating a third secure container comprising a fourth set of rules,
 - storing said third secure container at said second site,
 - communicating said third secure container from said second site to said first site,
 - storing said third secure container at said first site,
 - transferring said copied first portion of said first protected file from said first secure container to said third secure container,
 - transferring said third set of rules to said third secure container, and
 - communicating said third secure container containing said first portion of said first protected file and said third set of rules from said first site to said second site.

37. A method as in claim 36 in which said step of storing said copied first portion and said third set of rules in said second secure container further comprises storing said third secure container in said second secure container.

38. A method as in claim 36 in which said step of storing said copied first portion and said third set of rules in said second secure container further comprises:

- removing said copied first portion from said third secure container and transferring said copied first portion to said second secure container; and
- removing said third set of rules from said third secure container and transferring said third set of rules to said second secure container.

39. A method as in claim 38 in which said step of transferring said third set of rules to said second secure container further comprises creating a fourth set of rules.

40. A method as in claim 39 further comprising use of said fourth set of rules to govern at least one aspect of use of said copied first portion.

41. A method comprising performing the following steps within a virtual distribution environment comprising one or more electronic appliances and a first secure container, said first secure container comprising (a) a first control set, and (b) a second secure container

comprising a second control set and first protected information:

- using at least one control from said first control set or said second control set to govern at least one aspect of use of said first protected information while said first protected information is contained within said first secure container;
- creating a third secure container comprising a third control set for governing at least one aspect of use of protected information contained within said third secure container;
- incorporating a first portion of said first protected information in said third secure container, said first portion made up of some or all of said first protected information; and
- using at least one control to govern at least one aspect of use of said first portion of said first protected information while said first portion is contained within said third secure container.

42. A method as in claim 41, in which said first secure container further includes a fourth secure container comprising a fourth control set and second protected information and further comprising the following step:

- using at least one control from said first control set or said fourth control set to govern at least one aspect of use of said second protected information while said second protected information is contained within said first secure container.

43. A method as in claim 41, in which said step of creating a third secure container includes:

- creating said third control set by incorporating at least one control from said first control set.

44. A method as in claim 43, in which said step of incorporating at least one control from said first control set is accomplished in a secure manner.

45. A method as in claim 41, in which said step of creating a third secure container includes:

- creating said third control set by incorporating at least one control from said second control set.

46. A method as in claim 45, in which said step of incorporating at least one control from said second control set is accomplished in a secure manner.

47. A method as in claim 41, in which said step of creating a third secure container includes:

- creating said third control set by incorporating at least one control not found in said first control set or said second control set.

48. A method as in claim 47 in which said step of incorporating at least one control not found in said first control set or said second control set is accomplished in a secure manner.

49. A method as in claim 41, in which said step of creating a third secure container is governed at least in part by at least one control contained within said first control set.

50. A method as in claim 41, in which said step of creating a third secure container is governed at least in part by at least one control contained within said second control set.

51. A method as in claim 41 in which said step of creating a third

secure container is governed at least in part by at least one control not contained within said first control set or said second control set.

52. A method as in claim 41 in which said step of creating a third secure container occurs at a first site, and further comprising:

- copying or transferring said third secure container from said first site to a second site located remotely from said first site.

53. A method as in claim 52 in which said first site is associated with a content distributor.

54. A method as in claim 53 in which said second site is associated with a user of content.

55. A method as in claim 54 further comprising the following step:

- said user directly or indirectly initiating communication with said first site.

56. A method as in claim 55 in which said step of said user directly or indirectly initiating communication with said first site includes

- transmitting a fourth secure container to said first site, said fourth secure container comprising a fourth control set.

57. A method as in claim 56 in which said fourth control set includes at least a REGISTER control.

58. A method as in claim 56 in which said fourth control set includes at least a WANT control.

59. A method as in claim 56 in which said fourth control set includes one or more controls specifying content desired by said user and terms under which said user is willing to obtain said content.

60. A method as in claim 56 in which said step of creating said third secure container is governed, at least in part, by at least one control from said fourth control set.

61. A method as in claim 56 in which said third control set includes one or more controls created at least in part through an interaction among said first control set, said second control set and said fourth control set.

62. A method as in claim 56 in which said third control set includes at least one control incorporated from said first control set, one control incorporated from said second control set and one control incorporated from said fourth control set.

63. A method as in claim 56 in which said third control set includes at least one control not found in said first control set, said second control set or said fourth control set.

64. A method as in claim 54 in which said third control set includes one or more controls at least in part governing the use by said user of at least a portion of said first portion of said first protected information.

65. A method as in claim 64 in which said third control set includes one or more controls at least in part governing the price to be paid by said user for use of at least a portion of said first portion of said first protected information.

66. A method as in claim 64 in which said third control set includes one or more controls at least in part governing or specifying an auditing method to be used in connection with use by said user of at least a portion of said first portion of said first protected information.

67. A method as in claim 66 wherein at least some auditing performed in accordance with said auditing method is performed at said second site.

68. A method as in claim 66 in which said third control set includes one or more controls at least in part specifying one or more allowed clearinghouses to receive payment information from said

user for use of at least a portion of said first portion of said first protected information.

69. A method as in claim 66 in which said third control set includes one or more controls at least in part specifying information to be provided by said user in return for use of at least a portion of said first portion of said first protected information.

70. A method as in claim 69 further comprising the step of:

- encrypting at least a portion of said information to be provided by said user.

71. A method as in claim 52 further comprising

- establishing a level of compensation required for at least one of (a) said copying or transferring step, or (b) at least one aspect of use at said second site of at least a portion of said first portion of said first protected information, and
- calling a budget method to establish whether one or more budgets associated with said user are sufficient to satisfy said required compensation.

72. A method as in claim 71 further comprising

- blocking said copying or transferring step and/or said at least one aspect of use if said budget method establishes that said one or more budgets associated with said user are not sufficient to satisfy said required compensation.

73. A method as in claim 71 in which said budget method is governed at least in part by one or more controls contained in said first control set.

74. A method as in claim 71 in which said budget method is governed at least in part by one or more controls contained in said second control set.

75. A method as in claim 74 in which said budget method is also governed at least in part by one or more controls contained in said first control set.

76. A method as in claim 41 in which said creation of said third secure container further comprises using a template which specifies one or more of the controls contained in said third control set.

77. A method as in claim 49 in which said creation of said third secure container further comprises using a template which specifies one or more attributes of said third secure container.

78. A method as in claim 52 in which said creation of said third secure container further comprises using a template which specifies one or more of the controls contained in said third control set.

79. An electronic appliance comprising:

- a memory storing:
- a first secure container comprising a first rule set and first protected information, and
- a second secure container comprising a second rule set, said first secure container being stored within said second secure container;
- a secure processing unit comprising:
 - means for creating a third secure container comprising a third rule set, said means further comprising:
 - means for copying and/or removing at least one rule from said first rule set or said second rule set; and
 - means for incorporating said at least one rule in said third rule set;
- means by which at least one rule from said first rule set or

said second rule set governs, at least in part, said means for creating a third secure container;

- means for extracting at least a first portion of said first protected information from said first secure container; and
- means for copying or transferring said first portion of said first protected information from said first secure container to said third secure container;
- said means for copying or transferring operating at least in part under the control of said first rule set and/or said second rule set.

80. An electronic appliance as in claim 79 further comprising means by which at least one rule from said first or second rule set is incorporated in said third rule set.

81. A data processing arrangement comprising:

- a first secure container comprising first protected information and a first rule set governing use of said first protected information;
- a second secure container comprising a second rule set;
- means for creating and storing a third secure container; and
- means for copying or transferring at least a portion of said first protected information and a third rule set governing use of said portion of said first protected information to said second secure container, said means for copying or transferring comprising:
 - means for incorporating said third secure container within said second secure container.

82. A data processing arrangement as in claim 81 further comprising:

- means for applying at least one rule from said third rule set to at least in part govern at least one factor related to use of said portion of said first protected information.

83. A data processing arrangement as in claim 82 further comprising:

- means for applying at least one rule from said second rule set to at least in part govern at least one factor related to use of said portion of said first protected information.

84. A data processing arrangement as in claim 82 in which:

- said third rule set includes at least one rule from said first rule set.

85. A method comprising the following steps:

- creating a first secure container comprising a first rule set and first protected information;
- storing said first secure container in a first memory;
- creating a second secure container comprising a second rule set;
- storing said second secure container in a second memory;
- copying or transferring at least a first portion of said first protected information to said second secure container, said copying or transferring step comprising:
 - creating a third secure container comprising a third

- rule set;
- o copying said first portion of said first protected information;
- o transferring said copied first portion of said first protected information to said third secure container; and
- o copying or transferring said copied first portion of said first protected information from said third secure container to said second secure container.

86. A method as in claim 85 wherein said steps of creating said second secure container, creating said third secure container, and copying said first portion of said first protected information, are securely performed by one or more protected processing environments.

87. A method as in claim 85 in which said copied first portion of said first protected information consists of the entirety of said first protected information.

88. A method as in claim 85 in which said copied first portion of said first protected information consists of less than the entirety of said first protected information.

89. A method as in claim 85 in which

- said first memory is located at a first site,
- said second memory is located at a second site remote from said first site, and
- said step of copying or transferring said first portion of said first protected information to said second secure container further comprises copying or transferring said third secure container from said first site to said second site.

90. A method as in claim 85 in which

- said first memory and said second memory are located at the same site.

91. A method as in claim 90 in which

- said first memory comprises first addressable memory locations, and
- said second memory comprises second addressable memory locations in the same address space as said first addressable memory locations.

92. A method as in claim 91 in which

- said first addressable memory locations and said second addressable memory locations are located within the same physical memory device.

93. A method as in claim 85 in which

- said step of copying transferring said copied first portion of said first protected information from said third secure container to said second secure container further comprises storing said third secure container in said second secure container.

94. A method as in claim 85 further comprising:

- creating a fourth rule set.

95. A method as in claim 94 further comprising:

- using said fourth rule set to govern at least one aspect of use of said copied first portion of said first protected information.

96. A method comprising performing the following steps within a virtual distribution environment comprising one or more electronic appliances and a first secure container, said first secure container comprising a first control set and first protected information:

- using at least one control from said first control set to govern at least one aspect of use of said first protected information while said first protected information is contained within said first secure container;
- creating a second secure container comprising a second control set for governing at least one aspect of use of protected information contained within said second secure container;
- incorporating a first portion of said first protected information in said second secure container, said first portion made up of some or all of said first protected information;
- using at least one control to govern at least one aspect of use of said first portion of said first protected information while said first portion is contained within said second secure container; and
- incorporating said second secure container containing said first portion of said first protected information within a third secure container comprising a third control set.

97. An electronic appliance comprising:

- a memory storing:
 - a first secure container comprising a first rule set and first protected information, and
 - a second secure container comprising a second rule set;
- a secure processing unit comprising:
 - means for creating a third secure container comprising a third rule set, said means further comprising:
 - means for copying and/or removing at least one rule from said first rule set; and
 - means for incorporating said at least one rule in said third rule set;
 - means by which at least one rule from said first rule set governs, at least in part, said means for creating said third secure container;
 - means for extracting at least a first portion of said first protected information from said first secure container;
 - means for copying or transferring said first portion of said first protected information from said first secure container to said third secure container;
 - said means for transferring operating at least in part under the control of said first rule set and/or said third rule set; and
 - means for incorporating said third secure container within said second secure container.

98. A method as in claim 1 further comprising

- calling a method to govern, at least in part, the creation of

said second set of controls.

99. A method as in claim 1 in which said first protected content file includes attribute data.

100. A method as in claim 2 in which said first protected content file includes classification data.

101. A method as in claim 3 in which said first protected content file comprises attribute data.

This is a divisional of application Ser. No. 08/388,107, filed Feb. 13, 1995, abandoned.

Background/Summary:

Show background/summary

Drawing

Show drawing descriptions

Descriptions:

Description of

Show description of preferred embodiments

Preferred

Embodiments:

Foreign References:

Publication	Country	Date	IPC Class
<u>BE1984000900479</u>	Belgium	12 /1984	
<u>EP1983000084441</u>	European Patent Office (EPO)	7 /1983	
<u>EP1984000128672</u>	European Patent Office (EPO)	12 /1984	
<u>EP19850A0135422</u>	European Patent Office (EPO)	3 /1985	
<u>EP1986000180460</u>	European Patent Office (EPO)	5 /1986	
<u>EP1988000370146</u>	European Patent Office (EPO)	11 /1988	
<u>EP19900399822A2</u>	European Patent Office (EPO)	11 /1990	
<u>EP19910421409A2</u>	European Patent Office (EPO)	4 /1991	
<u>EP19910456386A2</u>	European Patent Office (EPO)	11 /1991	
<u>EP19920469864A2</u>	European Patent Office (EPO)	2 /1992	
<u>EP19930565314A2</u>	European Patent Office (EPO)	10 /1993	
<u>EP19940593305A2</u>	European Patent Office (EPO)	4 /1994	
<u>EP19950651554A1</u>	European Patent Office (EPO)	5 /1995	
<u>EP19950668695A2</u>	European Patent Office (EPO)	8 /1995	
<u>EP1996000725376</u>	European Patent Office (EPO)	1 /1996	
<u>EP19960696798A1</u>	European Patent Office (EPO)	2 /1996	
<u>EP19960695985A1</u>	European Patent Office (EPO)	2 /1996	
<u>EP19960715247A1</u>	European Patent Office (EPO)	6 /1996	
<u>EP19960715246A1</u>	European Patent Office (EPO)	6 /1996	
<u>EP19960715245A1</u>	European Patent Office (EPO)	6 /1996	
<u>EP19960715244A1</u>	European Patent Office (EPO)	6 /1996	
<u>EP19960715243A1</u>	European Patent Office (EPO)	6 /1996	
<u>EP19960749081A1</u>	European Patent Office (EPO)	12 /1996	
<u>EP19970778513A2</u>	European Patent Office (EPO)	6 /1997	
<u>EP19970795873A2</u>	European Patent Office (EPO)	9 /1997	
<u>DE1990038039821</u>	Germany	1 /1990	
<u>JP1982000000726</u>	Japan	5 /1982	

<u>JP1987000241061</u>	Japan	10 /1987	
<u>JP1989000068835</u>	Japan	3 /1989	
<u>JP1989000068835</u>	Japan	3 /1989	
<u>JP1990000242352</u>	Japan	9 /1990	
<u>JP1990000247763</u>	Japan	10 /1990	
<u>JP1990000294855</u>	Japan	12 /1990	
<u>JP1992000369068</u>	Japan	12 /1992	
<u>JP1993000181734</u>	Japan	7 /1993	
<u>JP1993000257783</u>	Japan	10 /1993	
<u>JP1993000268415</u>	Japan	10 /1993	
<u>JP1994000001757</u>	Japan	6 /1994	
<u>JP1994006225059</u>	Japan	8 /1994	
<u>JP1994000215010</u>	Japan	8 /1994	
<u>JP1995000084852</u>	Japan	3 /1995	
<u>JP1995000056794</u>	Japan	3 /1995	
<u>JP1995000141138</u>	Japan	6 /1995	
<u>JP1995000200492</u>	Japan	8 /1995	
<u>JP1995000200317</u>	Japan	8 /1995	
<u>JP1995000244639</u>	Japan	9 /1995	
<u>JP1996000137795</u>	Japan	5 /1996	
<u>JP1996000152990</u>	Japan	6 /1996	
<u>JP1996000185298</u>	Japan	7 /1996	
<u>GB1984002136175</u>	United Kingdom	9 /1984	
<u>GB1993002264796</u>	United Kingdom	9 /1993	
<u>GB1996002294348</u>	United Kingdom	4 /1996	
<u>GB1996002295947</u>	United Kingdom	6 /1996	
<u>WO1985WOA8502310</u>	World Intellectual Property Organization (WIPO)	5 /1985	
<u>WO1985WO0003584</u>	World Intellectual Property Organization (WIPO)	8 /1985	
<u>WO1990WO0002382</u>	World Intellectual Property Organization (WIPO)	3 /1990	
<u>WO1992WO0006438</u>	World Intellectual Property Organization (WIPO)	4 /1992	
<u>WO1992WO0022870</u>	World Intellectual Property Organization (WIPO)	12 /1992	
<u>WO1993WO0001550</u>	World Intellectual Property Organization (WIPO)	1 /1993	
<u>WO1994WO0001821</u>	World Intellectual Property Organization (WIPO)	1 /1994	
<u>WO1994WO0003859</u>	World Intellectual Property Organization (WIPO)	2 /1994	
<u>WO1994WO0006103</u>	World Intellectual Property Organization (WIPO)	3 /1994	
<u>WO1994WO0016395</u>	World Intellectual Property Organization (WIPO)	7 /1994	

WO1994WO0018620	World Intellectual Property Organization (WIPO)	8 /1994	
WO1994WO0022266	World Intellectual Property Organization (WIPO)	9 /1994	
WO1994WO0027406	World Intellectual Property Organization (WIPO)	11 /1994	
WO1995WO0014289	World Intellectual Property Organization (WIPO)	6 /1995	
WO1996WO0000963	World Intellectual Property Organization (WIPO)	1 /1996	
WO1996WO0006503	World Intellectual Property Organization (WIPO)	2 /1996	
WO1996WO0003835	World Intellectual Property Organization (WIPO)	2 /1996	
WO1996WO0005698	World Intellectual Property Organization (WIPO)	2 /1996	
WO1996WO0013013	World Intellectual Property Organization (WIPO)	5 /1996	
WO1996WO0021192	World Intellectual Property Organization (WIPO)	7 /1996	
WO1997WO0003423	World Intellectual Property Organization (WIPO)	1 /1997	
WO1997WO0007656	World Intellectual Property Organization (WIPO)	3 /1997	
WO1997WO0032251	World Intellectual Property Organization (WIPO)	9 /1997	
WO1997WO0048203	World Intellectual Property Organization (WIPO)	12 /1997	

Other References:
Article info links by

ISI

THOMSON SCIENTIFIC

- Applications Requirements for Innovative Video Programming; How to Foster (or Cripple) Program Development Opportunities for Interactive Video Programs Delivered on Optical Media; A Challenge for the Introduction of DVD (Digital Video Disc) (Oct. 19-20, 1995, Sheraton Universal Hotel, Universal City CA).
- Arneke, David, et al., News Release, AT&T, Jan. 9, 1995, AT&T encryption system protects information services, 1 page.
- AT&T Technology, vol. 9, No. 4, New Products, Systems and Services, pp. 16-19, Undated.
- Barassi, Theodore Sedgwick, Esq., The Cybernotary: Public Key Registration and Certification and Authentication of International Legal Transactions, 4 pages, Undated.
- Bruner, Rick E., PowerAgent, NetBot help advertisers reach Internet shoppers, Aug. 1997 (Document from Internet).
- CD ROM, Introducing . . . The Workflow CD-ROM Sampler, Creative Networks, MCIMail: Creative Networks, Inc., Palo Alto, California, Undated.
- Clark, Tim, Ad service gives cash back, www.news.com, Aug. 4, 1997, 2 pages (Document from Internet).
- Communications of the ACM, Jun. 1996, vol. 39, No. 6.
- Cunningham, Donna, et al., News Release, AT&T, Jan. 31, 1995, AT&T, VLSI Technology join to improve info highway security, 3 pages.
- Data Sheet, About the Digital Notary Service, Surety Technologies, Inc., 1994-95, 6 pages.
- Dempsey, et al., D-Lib Magazine, Jul./Aug. 1996 The Warwick Metadata Workshop: A Framework for the Deployent of Resource Description, Jul. 15, 1996.
- Document from Internet, cgi@ncsa.uiuc.edu, CGI Common Gateway Interface, 1 page, 1996.
- Firefly Network, Inc., www.ffly.com, What is Firefly? Firefly revision: 41.4 Copyright 1995, 1996.
- Gleick, James, "Dead as a Dollar" The New York Times Magazine, Jun. 16,

- 1996, Section 6, pp. 26-30, 35, 42, 50, 54.
- Greguras, Fred, Softic Symposium '95, Copyright Clearances and Moral Rights, Nov. 30, 1995 (as updated Dec. 11, 1995), 3 pages.
- Harman, Harry H., Modern Factor Analysis, Third Edition Revised, University of Chicago Press Chicago and London, Third revision published 1976.
- Herzberg, Amir et al., Public Protection of Software, ACM Transactions on Computer Systems, vol. 5, No. 4, Nov. 1987, pp. 371-393. (23 pages)
- Holt, Stannie, Start-up promises user confidentiality in Web marketing service, Info World Electric, Aug. 13, 1997 (Document from Internet).
- Hotjava.TM.: The Security Story, 4 pages, Undated.
- Invoice? What is an Invoice? Business Week, Jun. 10, 1996.
- Javasoft, Frequently Asked Questions--Applet Security, What's Java.TM.? Products and Services, Java/Soft News, Developer's Cornier, Jun. 7, 1996, 8 pages.
- Jiang, et al, A concept-Based Approach to Retrieval from an Electronic Industrial Directory, International Journal of Electronic Commerce, vol. 1, No. 1, Fall 1996, pp. 51-72.
- Jones, Debra, Top Tech Stories, PowerAgent Introduces First Internet 'Infomediary' to Empower and Protect Consumers, Aug. 13, 1997 3 pages (Document from Internet).
- Kohntopp, M., Sag's durch die Blume, Apr. 1996, marit@schulung.netuse.de.
- Lagoze, Carl, D-Lib Magazine, Jul./Aug. 1996, The Warwick Framework, A Container Architecture for Diverse Sets of Metadata.
- MacLachlan, Malcolm, PowerAgent Debuts Spam-Free Marketing, TechWire, Aug. 13, 1997, 3 pages (Document from Internet), Undated.
- Milbrandt, E., Stenography Info and Archive, 1996.
- Mossberg, Walter S., Personal Technology, Threats to Privacy On-Line Become More Worrisome, Wall Street Journal, Oct. 24, 1996.
- Negroponte, Electronic Word of Mouth, Wired Oct. 1996, p. 218.
- News Release, Premenos Announces Templar 2.0--Next Generation Software for Secure Internet EDI, webmaster@templar.net, 1 page, Jan. 17, 1996.
- News Release, The Document Company Xerox, Xerox Announces Software Kit for Creating Working Documents with Dataglyphs, Nov. 6, 1995, Minneapolis, MN, 13 pages.
- PowerAgent Inc., Proper Use of Consumer Information on the Internet White Paper, Jun. 1997, Document from Internet, 9 pages (Document from Internet).
- PowerAgent Press Releases, What the Experts are Reporting on PowerAgent, Aug. 13, 1997, 6 pages (Document from Internet).
- PowerAgent Press Releases, What the Experts are Reporting on PowerAgent, Aug. 4, 1997, 5 pages (Document from Internet).
- PowerAgent Press Releases, What the Experts are Reporting on PowerAgent, Aug. 13, 1997, 3 pages (Document from Internet).
- Premenos Corp. White Paper: The Future of Electronic Commerce, A Supplement to Midrange Systems, Internet webmaster@premenos.com, 4 pages, Undated.
- Resnick, et al., Recommender Systems, Communications of the ACM, vol. 40, No. 3, Mar. 1997, pp. 56-89. (3 pages) [13 patents reference this \[Article info\]](#)
- Rothstein, Edward, The New York Times, Technology, Connections, Making the Internet come to you, through 'push' technology . . . p. D5, Jan. 20, 1997.
- Rutkowski, Ken, PowerAgent Introduces First Internet 'Infomediary' to Empower and Protect Consumers, Tech Talk News Story, Aug. 4, 1997 (Document from Internet).
- Sager, Ira (Edited by), Bits & Bytes, Business Week, Sep. 23, 1996, p. 142E.
- Schurmann, Jurgen, Pattern Classification, A Unified View of Statistical and Neural Approaches, John Wiley & Sons, Inc., 1996.
- Special Report, The Internet: Fulfilling the Promise The Internet: Bring Order From Chaos; Lynch, Clifford, Search the Internet; Resnick, Paul, Filtering Information on the Internet; Hearst, Marti A., Interfaces for Searching the Web; Stefik, Mark, Trusted Systems; Scientific American, Mar. 1997, pp. 49-

- 56, 62-64, 68-72, 78-81.
- Stefik, Mark, Introduction to Knowledge Systems, Chapter 7, Classification, pp. 543-607, 1995 by Morgan Kaufmann Publishers, Inc.
- Templar Overview,: Premenos, Internet info@templar.net, 4 pages, Undated.
- Templar Software and Services: Secure, Reliable, Standards-Based EDI Over the Internet, Premenos, Internet info@templar.net, 1 page, Undated.
- Voight, Joan, Beyond the Banner, Wired, Dec. 1996, pp. 196, 200, 204.
- Vonder Haar, Steven, PowerAgent Launches Commercial Service, Inter@ctive Week, Aug. 4, 1997 (Document from Internet).
- Weber, Dr. Robert, Digital Rights Management Technologies, A Report to the International Federation of Reproduction Rights Organisations, Oct. 1995, pp. 1-49.
- Weber, Dr. Robert, Digital Rights Management Technologies, Oct. 1995, 21 pages.
- Wepin Store, Stenography (Hidden Writing) (Common Law 1995).
- World Wide Web FAQ, How can I put an access counter on my home page?, 1 page, 1996.
- Yellin, F. Low Level Security in Java, 8 pages, Undated.
- IBM Technical Disclosure Bulletin, "Multimedia Mixed Object Envelopes Supporting a Graduated Fee Scheme via Encryption," vol. 37, No. 03, Mar. 1994, Armonk, NY.
- IBM Technical Disclosure Bulletin, "Transformer Rules for Software Distribution Mechanism-Support Products," vol. 37, No. 04B, Apr. 1994, Armonk, NY.
- Suida, Karl, Mapping New Applications onto New Technologies, "Security Services in Telecommunications Networks," Mar. 8-10, 1988, Zurich.
- Portland Software's ZipLock, Internet information, Copyright Portland Software 1996-1997, 12 pages.
- Dyson, Esther, "Intellectual Value," Wired Magazine, Jul. 1995, pp. 136-141 and 182-184.
- Argent Information Q&A Sheet, <http://www.digital-watermark.com/>, Copyright 1995, The Dice Company, 7 pages.
- Guillou, L.: "Smart Cards and Conditional Access", pp. 480-490 Advances in Cryptography, Proceedings of EuroCrypt 84 (Beth et al, Ed., Springer-Verlag 1985).
- Rankine, G., "Thomas--A Complete Single-Chip RSA Device," Advances in Cryptography, Proceedings of Crypto 86, pp. 480-487 (A.M. Odlyzko Ed., Springer-Verlag 1987). (8 pages)
- DSP56000/DSP56001 Digital Signal Processor User's Manual, Motorola, 1990, p. 2-2.
- Duse, Stephen R. and Burton S. Kaliski "A Cryptographic Library for the Motorola 56000" in Damgard, I. M., Advances in Cryptology--Proceedings Eurocrypt 90, Springer-Verlag, 1991, pp. 230-244. (15 pages) 16 patents reference this [Article info]
- Struif, Bruno "The Use of Chipcards for Electronic Signatures and Encryption" in : Proceedings for the 1989 Conference on VSLI and Computer Peripherals, IEEE Computer Society Press, 1989, pp. 4/155-4/158.
- Ryoichi Mori and Masaji Kawahara, The Transactions of the EIEICE, V. "Superdistribution: The Concept and the Architecture," E73 (Jul. 1990), No. 7, Tokyo, Japan.
- Stefik, "Internet Dreams: Archetypes, Myths, and Metaphors, Letting Loose the Light: Igniting Commerce in Electronic Publication," pp. 219-253, (1996) Massachusetts Institute of Technology.
- Stefik, Mark, "Letting Loose the Light, Igniting Commerce in Electronic Publication," (1994, 1995) Palo Alto, California.
- Shear, "Solutions for CD-ROM Pricing and Data Security Problems", pp. 530-533, CD ROM Yearbook 1988-1989 (Microsoft Press 1988 or 1989).
- Press Release, "National Semiconductor and EPR Partner For Information Metering/Data Security Cards" (Mar. 4, 1994).
- "Electronic Publishing Resources Inc. Protecting Electronically Published Properties Increasing Publishing Profits" (Electronic Publishing Resources, 1991).

- "The Benefits of ROI For Database Protection and Usage Based Billing" (Personal Library Software, 1987 or 1988).
- ROI-Solving Critical Electronic Publishing Problems (Personal Library Software, 1987 or 1988).
- Weber, "Metering Technologies for Digital Intellectual Property, A Report to the International Federation of Reproduction Rights Organisations," pp. 1-29; Oct. 1994, Boston, MA, USA.
- ROI (Personal Library Software, 1987 or 1988).
- DiscStore (Electronic Publishing Resources 1991).
- Yee, "Using Secure Coprocessors," CMU-CS-94-149, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA 15213, Undated.
- Tygar et al., "Dyad: A System for Using Physically Secure Coprocessors," School of Computer Science, Carnegie Mellon University, Pittsburgh, PA 15213 (undated).
- Tygar et al., "Dyad: A System for Using Physically Secure Coprocessors," School of Computer Science, Carnegie Mellon University, Pittsburgh, PA 15213 (May 1991).
- Maxemchuk, "Electronic Document Distribution," AT&T Bell Laboratories, Murry Hill, New Jersey 07974, Undated.
- Choudhury, et al., "Copyright Protection for Electronic Publishing over Computer Networks," AT&T Bell Laboratories, Murray Hill, New Jersey 07974 (Jun. 1994).
- Weingart, "Physical Security for the μ ABYSS System," IBM Thomas J. Watson Research Center, Yorktown Heights, New York 10598 (1987).
- White, "ABYSS: A Trusted Architecture for Software Protection," IBM Thomas J. Watson Research Center, Yorktown Heights, New York 10598 (1987).
- Neumann, et al., "A Provably Secure Operating System: The System, Its Applications, and Proofs," Computer Science Laboratory Report CSL-116, Second Edition, SRI International (May 1980).
- Caruso, "Technology, Digital Commerce 2 plans for watermarks, which can bind proof of authorship to electronic works," New York Times (Aug. 1995).
- "Electronic Currency Requirements, XIWT (Cross Industry Working Group)," no date.
- "NII, Architecture Requirements, XIWT," no date.
- Arthur K. Reilly, Standards committee T1-Telecommunications, Input to the 'International Telecommunications Hearings,' Panel 1: Component Technologies of the NII/GII, no date.
- Dan Bart, Comments in the Matter of Public Hearing and Request for Comments on the International Aspects of the National Information Infrastructure, Aug. 12, 1994.
- "Open System Environment Architectural Framework for National Information Infrastructure Services and Standards, in Support of National Class Distributed Systems," Distributed System Engineering Program Sponsor Group, Draft 1.0. Aug. 5, 1994.
- "Information Infrastructure Standards Panel: NII 'The Information Superhighway'," NationsBank--HGDeal--ASC X9, 15 pages, Undated.
- Jud Hofmann, "Interfacing the NII to User Homes," Electronic Industries Association, Consumer Electronic Bus Committee, 14 slides, no date.
- "Framework for National Information Infrastructure Services," NIST, Jul. 1994, 12 slides.
- Claude Baggett, "Cable's Emerging Role in the Information Superhighway," Cable Labs, 13 slides, Undated.
- "IISP Break Out Session Report for Group No. 3, Standards Development and Tracking System," no date.
- "XIWT Cross Industry Working Team," 5 pages, Jul. 1994.
- "Computer Systems Policy Project (CSSP), Perspectives on the National Information Infrastructure: Ensuring Interoperability (Feb. 1994)," Feb. 1994.
- "Framework for National Information Infrastructure Services," Draft, U.S. Department of Commerce, Jul. 1994.
- "EIA and TIA White Paper on National Information Infrastructure," published by the Electronic Industries Association and the Telecommunications Industry Association, Washington, D.C., no date.

- Michael Baum, "Worldwide Electronic Commerce: Law, Policy and Controls Conference," program details, Nov. 11, 1993.
- Bruce Sterling, "Literary freeware: Not for Commercial Use," remarks at Computers, Freedom and Privacy Conference IV, Chicago, Mar. 26, 1994.
- "The 1:1 Future of the Electronic Marketplace: Return to a Hunting and Gathering Society," 2 pages, no date.
- D. Linda Garcia, testimony before a hearing on science, space and technology, May 26, 1994.
- Wired 1.02, "Is Advertising Really dead?, Part 2," 1994.
- Hugh Barnes, memo to Henry LaMuth, subject: George Gilder articles, May 31, 1994.
- Daniel J. Weitzner, A Statement on EFF's Open Platform Campaign as of Nov., 1993, 3 pages.
- "Serving the Community: A Public-Interest Vision of the National Information Infrastructure," Computer Professionals for Social Responsibility, Executive Summary, no date.
- Steven Schlossstein, International Economy, "America: The G7's Comeback Kid," Jun./Jul. 1993.
- Lance Rose, "Cyberspace and the Legal Matrix: Laws or Confusion?," 1991.
- "Cable Television and America's Telecommunications Infrastructure," National Cable Television Association, Apr. 1993.
- Adele Weder, "Life on the Infohighway," 4 pages, no date.
- T. Valovic, Telecommunications, "The Role of Computer Networking in the Emerging Virtual Marketplace," pp. 40-44, Undated.
- Dr. Joseph N. Pelton, Telecommunications, "Why Nicholas Negroponte is Wrong About the Future of Telecommunication," pp. 35-40, Jan. 1993.
- Nicholas Negroponte, Telecommunications, "Some Thoughts on Likely and expected Communications scenarios: A Rebuttal," pp. 41-42, Jan. 1993.
- Tom Stephenson, Advanced Imaging, "The Info Infrastructure Initiative: Data SuperHighways and You," pp. 73-74, May 1993.
- Steve Rosenthal, New Media, "Mega Channels," pp. 36-46, Sep. 1993.
- News Release, The White House, Office of the President, "Background on the Administration's Telecommunications Policy Reform Initiative," Jan. 11, 1994.
- Steve Rosenthal, New Media, "Interactive Network: Viewers Get Involved," pp. 30-31, Dec. 1992.
- Steve Rosenthal, New Media, "Interactive TV: The Gold Rush Is On," pp. 27-29, Dec. 1992.
- EFFector Online vol. 6 No. 6, "A Publication of the Electronic Frontier Foundation," 8 pages, Dec. 6, 1993.
- Mike Lanza, electronic mail, "George Gilder's Fifth Article--Digital Darkhorse--Newspapers," Feb. 21, 1994.
- Steven Levy, Wired, "E-Money, That's What I Want," 10 pages, Dec. 1994.
- Kevin Kelly, Whole Earth Review, "E-Money," pp. 40-59, Summer 1993.
- Green paper, "Intellectual Property and the National Information Infrastructure, a Preliminary Draft of the Report of the Working Group on Intellectual Property Rights," Jul. 1994.
- Communications of the ACM, "Intelligent Agents," Jul. 1994, vol. 37, No. 7.
- "Encapsulation: An Approach to Operating System Security," Bisbey, II et al., Oct. 1973, pp. 666-675.
- "Encryption Methods in Data Networks," Blom et al., Ericsson Technics, No. 2, 1978, Stockholm, Sweden.
- First CII Honeywell Bull International Symposium on Computer Security and Confidentiality, Jan. 26-28, 1981, Conference Text, pp. 1-21.
- Codercard, Spec Sheet--Basic Coder Subsystem, No date given.
- "Micro Card"--Micro Card Technologies, Inc., Dallas, Texas, No date given.
- "A Method of Software Protection Based on the Use of Smart Cards and Cryptographic Techniques," Schnaumueler-Bichl et al., No date given.
- I "The New Alexandria" No. 1, Alexandria Institute, pp. 1-12, Jul.-Aug. 1986.
- Denning et al., "Data Security," 11 Computing Surveys No. 3, Sep. 1979.
- Kent, "Protecting Externally Supplied Software In Small Computers"

(MIT/LCS/TR-255 Sep. 1980).

- Proceedings of the IEEE, vol. 67, No. 3, Mar. 1979, "Privacy and Authentication: An Introduction to Cryptography," Whitfield Diffie and Martin E. Hellman, pp. 397-427. (31 pages)
- Digest of Papers, VLSI: New Architectural Horizons, Feb. 1980, "Preventing Software Piracy With Crypto-Microprocessors," Robert M. Best, pp. 466-469.
- IEEE Transactions on Information Theory, vol. 22, No. 6, Nov. 1976, "New Directions in Cryptography," Whitfield Diffie and Martin E. Hellman, pp. 644-651. (11 pages)
- Low, et al., "Anonymous Credit Cards," AT&T Bell Laboratories, Proceedings of the 2nd ACM Conference on Computer and Communication Security, Fairfax, Virginia, Nov. 2-4, 1994.
- Tygar et al., "Cryptography: It's Not Just For Electronic Mail Anymore," CMU-CS-93-107, School of Computer Science Carnegie Mellon University, Pittsburgh, Pennsylvania, Mar. 1, 1993.
- Smith, et al., "Signed Vector Timestamps: A Secure Protocol for Partial Order Time," CMU-93-116, School of Computer Science Carnegie Mellon University, Pittsburgh, Pennsylvania, Oct. 1991; version of Feb. 1993.
- Kristol et al., "Anonymous Internet Mercantile Protocol," AT&T Bell Laboratories, Murray Hill, New Jersey, Draft: Mar. 17, 1994.
- Low et al., "Document Marking and Identification using both Line and Word Shifting," AT&T Bell Laboratories, Murray Hill, New Jersey, Jul. 29, 1994.
- Low et al., "Anonymous Credit Cards and its Collusion Analysis," AT&T Bell Laboratories, Murray Hill, New Jersey, Oct. 10, 1994.



Nominate this invention for the Gallery...

Alternative Searches

Browse


[Patent Number](#)


[Boolean Text](#)



[Advanced Text](#)


[U.S. Class by title](#)


[U.S. Class by number](#)


[IP Listing Search](#)


[IBM Technical Disclosure Bulletin](#)


[Derwent World Patents Index](#)


[disclosures@IP.Com](#)

[Privacy Policy](#) | [Terms & Conditions](#) | [Site Map](#) | [Help](#) | [Contact Us](#)

© 1997 - 2001 Delphion Inc.